



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,176	07/01/2005	Knut Brandrud	P14739-US1	5692
27045	7590	05/16/2007		
ERICSSON INC. 6300 LEGACY DRIVE M/S EVR 1-C-11 PLANO, TX 75024			EXAMINER PATEL, ASHOKKUMAR B	
			ART UNIT 2154	PAPER NUMBER
			MAIL DATE 05/16/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/517,176	BRANDRUD ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Ashok B. Patel	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 07 December 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) 1-14 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 15-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>12/7/04, 12/14/06</u> .                                       | 6) <input type="checkbox"/> Other: _____                          |

### DETAILED ACTION

1. Claims 1-23 are subject to examination. Claims 1-14 have been cancelled.

#### ***Claim Rejections - 35 USC § 101***

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim 23 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

#### **Referring to claim 23,**

Claim 23 recites a " Program unit loadable into a proxy server in a communication network, wherein the program unit comprises code adapted to store a cookie for a first web server:.....". At page 6, lines 27-28 of the instant specification contains intrinsic evidence as " It can also be embodied as a sequence of signals loadable into a web server, e.g. over a data link." As such, in the case of a sequence of signals loadable into a web server, e.g. over a data link", the "code" is merely electromagnetic signals or carrier waves which do not fall into any of the four statutory categories set forth in the above statute.

#### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention

Art Unit: 2154

was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claim 15-17, 19-21 and 23 are rejected under 35 U.S.C. 103(a) as being Unpatentable over Pilkington et al. (hereinafter Pilkington)(WO 01/78351 A2) in view of Lennie et al. (hereinafter Lennie) (US 6, 836, 845 B1)

**Referring to claim 15,**

Pilkington teaches method for providing access to information related to a client terminal (Fig. 8, element 31, page 14, step 92) to a first web server (Fig. 8, element 87, "WEB proxy is Web Server.), the information being stored by a second web server (Fig. 8, element 86, A second web server is "Authentication Server.), wherein the first web server (Fig. 8, element 87, "WEB proxy is Web Server.) is connected to the client terminal (Fig. 8, element 31) via a proxy server (Fig. 8, element 85 "WAP Gateway/Transcoder is a proxy server. Examiner understands the function of WAP Gateway as being a proxy server for the client terminal 31 since as stated in Step 92 on page 14.) , comprising the steps of:

storing a cookie for the first web server in said proxy server (Fig. 7, element "set Cookie" in Gateway 55, Fig. 9, element 914-Valid set/reset cookie"), wherein the cookie is related to the client (page 15, Step 914) and wherein the cookie is sent to the proxy server in a session according to a hypertext transfer protocol by the second web server (page 15, Step 914, "914 If the Security server 86 determines the credentials match then the Access control unit 87 sets a"cookie"on the transcoder 851 (or another part of the gateway 85) against the identity of the WAP phone 31, using HTML and HTTP. (If a

valid cookie already exists for the WAP phone, (see step 95), the latest access time recorded by the cookie is updated.");

receiving a message from said client terminal that is addressed to the first web server (Fig. 7, Element 672 "Add cookie" and page 14, Steps "98. The user enters a username and PIN along with the six-digit pseudo-random number shown on the token at that time. 99. The WAP Phone 31 sends the results of the page to the WAP Gateway 85 as a WML formatted response using WTP over IP. 910 The WAP Gateway 85 converts the WTP protocol to HTTP and passes the result to the Transcoder 851. 911 The Transcoder 851 converts the WML response to HTML and sends this on to the Access control unit 87 using HTTP. ");

inserting the cookie into the received message(Fig. 7, Element 672 "Add cookie", and forwarding the message to the first web server wherein said first web server uses said cookie for requesting said information from said second web server (page 14 and page 15, "95. The access control unit 87 checks whether there is a valid cookie associated with the request. If a valid cookie is found then the cookie is updated to reflect the new time of access (step 14) and the requested page is then returned as in step 15 below. If there is no cookie, (which will be the case if no previous access request has been made from the WAP phone 31, or if the time elapsed since the previous access time recorded for the cookie is longer than a timeout stated in the cookie configuration) the access control unit 87 identifies the request as one requiring a login, and returns a prompt page (in HTML over HTTP) to the transcoder 851, prompting for the Username and security codes: that is, the user's PIN and the pseudo-

Art Unit: 2154

random code currently shown on the token. 96. The Transcoder 851 receives the prompt page from the access control unit 87 and converts the HTML to WML and passes this page to the WAP Gateway 85. 97. The WAP Gateway 85 converts the HTTP protocol to WTP and delivers it to the WAP Phone 31 where it is displayed. 98. The user enters a username and PIN along with the six-digit pseudo-random number shown on the token at that time. 99. The WAP Phone 31 sends the results of the page to the WAP Gateway 85 as a WML formatted response using WTP over IP. 910 The WAP Gateway 85 converts the WTP protocol to HTTP and passes the result to the Transcoder 851. 911 The Transcoder 851 converts the WML response to HTML and sends this on to the Access control unit 87 using HTTP. 912 The Access control unit 87 checks the username, PIN and pseudo-random number against data stored in and generated by the Security server 86 to determine if the user should be authenticated. 913 If the details do not match, a rejection is sent back to the user as an HTML page which is translated by the Transcoder 851 and delivered through the WAP Gateway 85 to the phone 31, as in steps 95 to 912 above. This process is repeated either until the correct details are received or a maximum number of repetitions is exceeded. If the number of attempts exceeds the maximum the Security server 86 disables all entries for the username. 914 If the Security server 86 determines the credentials match then the Access control unit 87 sets a "cookie" on the transcoder 851 (or another part of the gateway 85) against the identity of the WAP phone 31, using HTML and HTTP. (If a valid cookie already exists for the WAP phone, (see step 95), the latest access time recorded by the cookie is updated.)

Pilkington fails to teach the cookie includes a network address of the second web server and said cookie identifying said second web server;

Lennie teaches at Fig. 9A, element 903, and at col. 10, line 1-5, "Cookie 900 of FIG. 9A also includes authentication and authorization system (AAS) server address 903. AAS server address 903 provides an address for accessing an authentication and authorization server that provides the desired information or service." (the cookie includes a network address of the second web server and said cookie identifying said second web server) and the application of Cookie for querying the for authentication and authorization system server 321 at col. 9, line 38-51, "Upon completion of registration, a cookie is provided as shown by step 813. In the embodiment shown in FIG. 6, a cookie is generated by registration server 340 and is transmitted from registration server 340 to client system 310. (33) In the embodiment shown in FIG. 7, all communications are routed through authentication and authorization system server 321. In this embodiment, registration (step 812) and providing a cookie (step 813) are provided through communication between palmtop computer 100 and server 321. The registration process and the generation of a cookie can be performed by either registration server 340 or authentication and authorization system server 321, or by distributing tasks between registration server 340 and authentication and authorization system server 321."

Therefore it would have been an obvious to one of an ordinary skill in art, having the teachings of Pilkington and Lennie in front of him at the time of invention was made, to incorporate Lennie's authentication and authorization system server 321's addressing

system such that the Internet address of the authentication and authorization system server is provided into the cookie to contact the authentication and authorization system server for user's credential match.

This would have been obvious because, as Lennie puts it at col. 10, line 1-7, "Cookie 900 of FIG. 9A also includes authentication and authorization system (AAS) server address 903. AAS server address 903 provides an address for accessing an authentication and authorization server that provides the desired information or service. This allows for load balancing to spread access across available authentication and authorization servers." versus having just one Authentication server of Fig. 8 in case Pilkington carrying the burden alone.

**Referring to claim 16,**

Pilkington teaches method according to claim 15, wherein the client terminal is a mobile terminal, the proxy server is at least one of a wireless application protocol gateway or a hypertext transfer protocol proxy server, and wherein the connection of the client terminal to the first web server further comprises the steps of: establishing a first connection between the client terminal and the proxy server according to a wireless application protocol or a hypertext transfer protocol; and establishing a second connection between the proxy server and the first web server according to a hypertext transfer protocol. (Page 15 Steps "99. The WAP Phone 31 sends the results of the page to the WAP Gateway 85 as a WML formatted response using WTP over IP. 910 The WAP Gateway 85 converts the WTP protocol to HTTP and passes the result to the



Transcoder 851. 911 The Transcoder 851 converts the WML response to HTML and sends this on to the Access control unit 87 using HTTP.”)

**Referring to claim 17,**

Pilkington teaches method according to claim 15 wherein said second web server includes an authentication server. (Fig. 5, element 56.)

**Referring to claim 19,**

Pilkington teaches proxy server for a communication network (Fig. 8, element 85 “WAP Gateway/Transcoder is a proxy server. Examiner understands the function of WAP Gateway as being a proxy server for the client terminal 31 since as stated in Step 92 on page 14.), wherein the proxy server comprises:

a memory for storing a cookie (Fig. 7, element “set Cookie” in Gateway 55, Fig. 9, element 914-Valid set/reset cookie”), said cookie associated with a particular client terminal (Fig. 8, element 31, page 14, step 92), page 15, Step 914, “914 If the Security server 86 determines the credentials match then the Access control unit 87 sets a “cookie” on the transcoder 851 (or another part of the gateway 85) against the identity of the WAP phone 31, using HTML and HTTP. (If a valid cookie already exists for the WAP phone, (see step 95), the latest access time recorded by the cookie is updated.”);

interfaces for sending and receiving messages with said client terminal (Fig. 8, element 31) and a first web server (Fig. 8, elements 87 is first Web server.); and

means for receiving a signal from said client terminal further comprising means for:

modifying said received signal to include said stored cookie(Fig. 7, Element 672 "Add cookie"); and

forwarding said modified signal to said first web server allowing said first web server to use said cookie to request said information from said second web server (page 14 and page 15, "95. The access control unit 87 checks whether there is a valid cookie associated with the request. If a valid cookie is found then the cookie is updated to reflect the new time of access (step 14) and the requested page is then returned as in step 15 below. If there is no cookie, (which will be the case if no previous access request has been made from the WAP phone 31, or if the time elapsed since the previous access time recorded for the cookie is longer than a timeout stated in the cookie configuration) the access control unit 87 identifies the request as one requiring a login, and returns a prompt page (in HTML over HTTP) to the transcoder 851, prompting for the Username and security codes: that is, the user's PIN and the pseudo-random code currently shown on the token. 96. The Transcoder 851 receives the prompt page from the access control unit 87 and converts the HTML to WML and passes this page to the WAP Gateway 85. 97. The WAP Gateway 85 converts the HTTP protocol to WTP and delivers it to the WAP Phone 31 where it is displayed. 98. The user enters a username and PIN along with the six-digit pseudo-random number shown on the token at that time. 99. The WAP Phone 31 sends the results of the page to the WAP Gateway 85 as a WML formatted response using WTP over IP. 910 The WAP Gateway 85 converts the WTP protocol to HTTP and passes the result to the Transcoder 851. 911 The Transcoder 851 converts the WML response to HTML and

Art Unit: 2154

sends this on to the Access control unit 87 using HTTP. 912 The Access control unit 87 checks the username, PIN and pseudo-random number against data stored in and generated by the Security server 86 to determine if the user should be authenticated. 913 If the details do not match, a rejection is sent back to the user as an HTML page which is translated by the Transcoder 851 and delivered through the WAP Gateway 85 to the phone 31, as in steps 95 to 912 above. This process is repeated either until the correct details are received or a maximum number of repetitions is exceeded. If the number of attempts exceeds the maximum the Security server 86 disables all entries for the username. 914 If the Security server 86 determines the credentials match then the Access control unit 87 sets a "cookie" on the transcoder 851 (or another part of the gateway 85) against the identity of the WAP phone 31, using HTML and HTTP. (If a valid cookie already exists for the WAP phone, (see step 95), the latest access time recorded by the cookie is updated.)

Pilkington fails to teach cookie including the network address identifying a second web server and cookie identifying said second web server

Lennie teaches at Fig. 9A, element 903, and at col. 10, line 1-5, "Cookie 900 of FIG. 9A also includes authentication and authorization system (AAS) server address 903. AAS server address 903 provides an address for accessing an authentication and authorization server that provides the desired information or service." (cookie including the network address identifying a second web server and cookie identifying said second web server) and the application of Cookie for querying the for authentication and authorization system server 321 at col. 9, line 38-51, "Upon completion of registration, a

Art Unit: 2154

cookie is provided as shown by step 813. In the embodiment shown in FIG. 6, a cookie is generated by registration server 340 and is transmitted from registration server 340 to client system 310. (33) In the embodiment shown in FIG. 7, all communications are routed through authentication and authorization system server 321. In this embodiment, registration (step 812) and providing a cookie (step 813) are provided through communication between palmtop computer 100 and server 321. The registration process and the generation of a cookie can be performed by either registration server 340 or authentication and authorization system server 321, or by distributing tasks between registration server 340 and authentication and authorization system server 321."

Therefore it would have been an obvious to one of an ordinary skill in art, having the teachings of Pilkington and Lennie in front of him at the time of invention was made, to incorporate Lennie's authentication and authorization system server 321's addressing system such that the Internet address of the authentication and authorization system server is provided into the cookie to contact the authentication and authorization system server for user's credential match.

This would have been obvious because, as Lennie puts it at col. 10, line 1-7, "Cookie 900 of FIG. 9A also includes authentication and authorization system (AAS) server address 903. AAS server address 903 provides an address for accessing an authentication and authorization server that provides the desired information or service. This allows for load balancing to spread access across available authentication and

Art Unit: 2154

authorization servers." versus having just one Authentication server of Fig. 8 in case Pilkington carrying the burden alone.

**Referring to claim 20,**

Pilkington teaches the server according to claim 19, wherein the client terminal is a mobile terminal, the proxy server is at least one of a wireless application protocol gateway or a hypertext transfer protocol proxy server, said server further comprising an interface means for establishing a connection between said client terminal with the first web server, wherein said interface means establishes a first connection between the client terminal and the server according to a wireless application protocol or a hypertext transfer protocol and establishes a second connection between the server and the first web server according to a hypertext transfer protocol. (Page 15 Steps "99. The WAP Phone 31 sends the results of the page to the WAP Gateway 85 as a WML formatted response using WTP over IP. 910 The WAP Gateway 85 converts the WTP protocol to HTTP and passes the result to the Transcoder 851. 911 The Transcoder 851 converts the WML response to HTML and sends this on to the Access control unit 87 using HTTP.")

**Referring to claim 21,**

Pilkington teaches the server according to claim 20 wherein said second web server includes an authentication server (Fig. 5, element 56).

**Referring to claim 23,**

Art Unit: 2154

Claim 23 is a claim to program unit loadable into a proxy server in a communication network carrying out the method in accordance with claim 15. Therefore claim 23 is rejected for the reasons set forth for claim 15.

5. Claims 18 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pilkington et al. (hereinafter Pilkington)(WO 01/78351 A2) in view of Lennie et al. (hereinafter Lennie) (US 6, 836, 845 B1), as applied to claims 15 and 19 above, and further in view of "MET Authorization for account based payment using, a SET Wallet Server" MET (MOBILE ELECTRONIC TRANSACTIONS) STANDARD, 'Online! 21 February 2001 (hereinafter Wallet Sever)

**Referring to claim 18,**

Keeping in mind the teachings of Pilkington and Lennie as applied to claim 15, both of these references fail to teach method according to claim 15 wherein said second web server includes a payment server for said client terminal.

Wallet server teaches method according to claim 15 wherein said second web server includes a payment server for said client terminal at page 12(15), Fig. 3, element "SET Wallet Server." (a payment server) for client terminal (page 12(15), Fig 3, element "PTD").

Therefore it would have been an obvious to one of an ordinary skill in art, having the teachings of Pilkington, Lennie and Wallet server in front of him at the time of invention was made, to incorporate Wallet server in the combined system of Pilkington and Lennie such that not only the client can be authenticated but also provided with a authorization mechanism to make payment online along with the authentication.

This would have been obvious because, as evident from line 1-8, page 15(15) of Wallet server that the client's authentication and payment authorization is presented to user every time the transaction is initiated by the client, the combined system will eliminate the cumbersome process required by Wallet server by including cookie stored at the proxy server of Pilkington for the contacting the appropriate servers as suggested by Linnie for authentication, and as suggested by Wallet server for payment authorization.

**Referring to claim 22,**

Keeping in mind the teachings of Pilkington and Lennie as applied to claim 15, both of these references fail to teach the server according to claim 20 wherein said second web server includes a payment server for said client terminal.

Wallet server teaches server according to claim 20 wherein said second web server includes a payment server for said client terminal at page 12(15), Fig. 3, element "SET Wallet Server." (a payment server) for client terminal (page 12(15), Fig 3, element "PTD").

Therefore it would have been an obvious to one of an ordinary skill in art, having the teachings of Pilkington, Lennie and Wallet server in front of him at the time of invention was made, to incorporate Wallet server in the combined system of Pilkington and Lennie such that not only the client can be authenticated but also provided with a authorization mechanism to make payment online along with the authentication.

This would have been obvious because, as evident from line 1-8, page 15(15) of Wallet server that the client's authentication and payment authorization is presented to

Art Unit: 2154

user every time the transaction is initiated by the client, the combined system will eliminate the cumbersome process required by Wallet server by including cookie stored at the proxy server of Pilkington for the contacting the appropriate servers as suggested by Linnie for authentication, and as suggested by Wallet server for payment authorization.

### ***Conclusion***

**Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 6:30 am-4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan A. Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Art Unit: 2154

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A handwritten signature in black ink, appearing to read 'Ashok B. Patel', with a stylized, cursive script.

Ashok B. Patel

Examiner

Art Unit 2154

\*\*\*